National Defense Industrial Association

Promoting National Security Since 1919

Cyber Security for Advanced Manufacturing

Protecting the Digital Thread

Software and Supply Chain Assurance (SSCA)
Spring Forum 2017
March 15, 2017

Michael McGrath
Consultant, Analytic Services Inc.
michael.mcgrath@anser.org

Continuation of Discussion Started at SSCA Winter 2016 Session

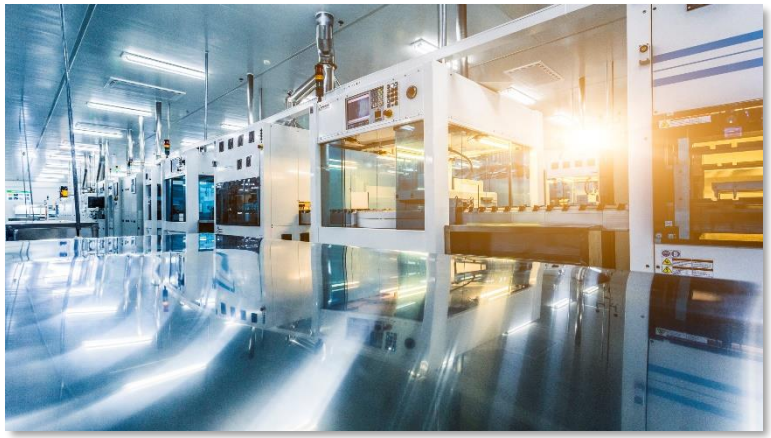
Dec 13, 2016 Confidentiality Session

- Bob Metzger (Rogers, Joseph, & O'Donnell)
  -- *"The 'Cyber' DFARS Requirements"*
- Vicki Michetti and Mary Thomas (DoD)
  -- *"Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations"*

Today –Implications for Manufacturing

- NDIA Joint Working Group focus:
  - Data protection and network protection (especially in the Operational Technology (OT) domain)
  - Throughout supply chain and across the life cycle
  - Confidentiality, Integrity, Availability

Advanced Manufacturing is a Cyber-physical Business



Increasingly digital

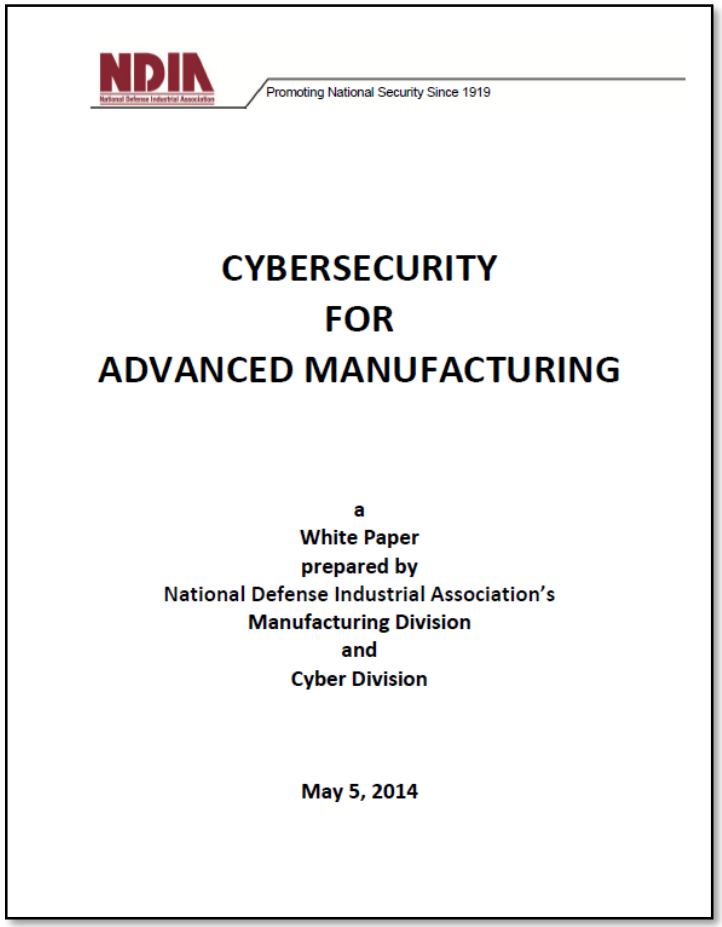
Smart Manufacturing

Industry 4.0

Industrial Internet of Things

- Networked at every level to gain efficiency, speed, quality and agility
- Constantly learning from models and data throughout the life cycle
- Driven by a "Digital Thread" of product and process information
  - Source of competitive advantage for manufacturers and their customers
  - Source of military advantage for DoD
  - Demands protection throughout the product lifecycle

NDIA White Paper: Protecting the Digital Thread



www.ndia.org/Divisions/Divisions/Manufacturing

Cyber risks in defense industrial base are national security concerns

Confidentiality	**Theft of technical info** -- can compromise national defense and economic security
Integrity	**Alteration of technical data** -- can alter the part or the process, with physical consequences to mission and safety
Availability	**Disruption or denial of process control** -- can shut down production and impact readiness

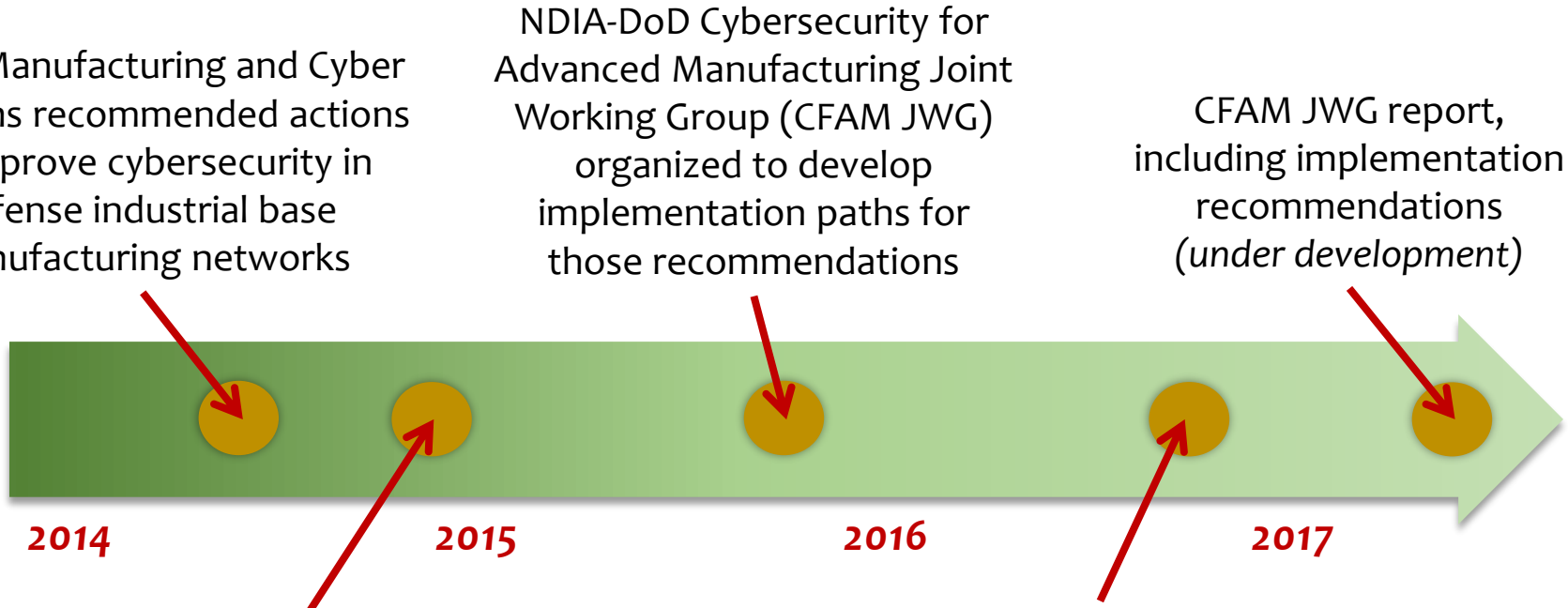
What We Heard from Interviews

Gov't, Industry, Academia (2014)

- CIOs/CISOs in the defense primes are implementing strong cyber risk management and sharing info through the DIB CS/IA and DSIE programs
  - *Concerned about suppliers and willing to work with them*
  - *Have not yet seen threat to factory systems, but acknowledge the possibility*
  - *Need cost/risk tradeoffs to arrive at an affordable solution*
- Industrial Control Systems (ICS) are soft targets. Culture differs from IT.
  - *Standards and guides* for ICS provide good risk management approaches. Implementation is spotty.*
- DoD has mandated protection of critical information
  - *Primes address in the program protection plan, but ICS security is not emphasized in DoD guidance*
- Defense R&D for cybersecurity is not currently focused on factory floor

*E.g. ANSI/ISA99 standards and NIST SP 800-82

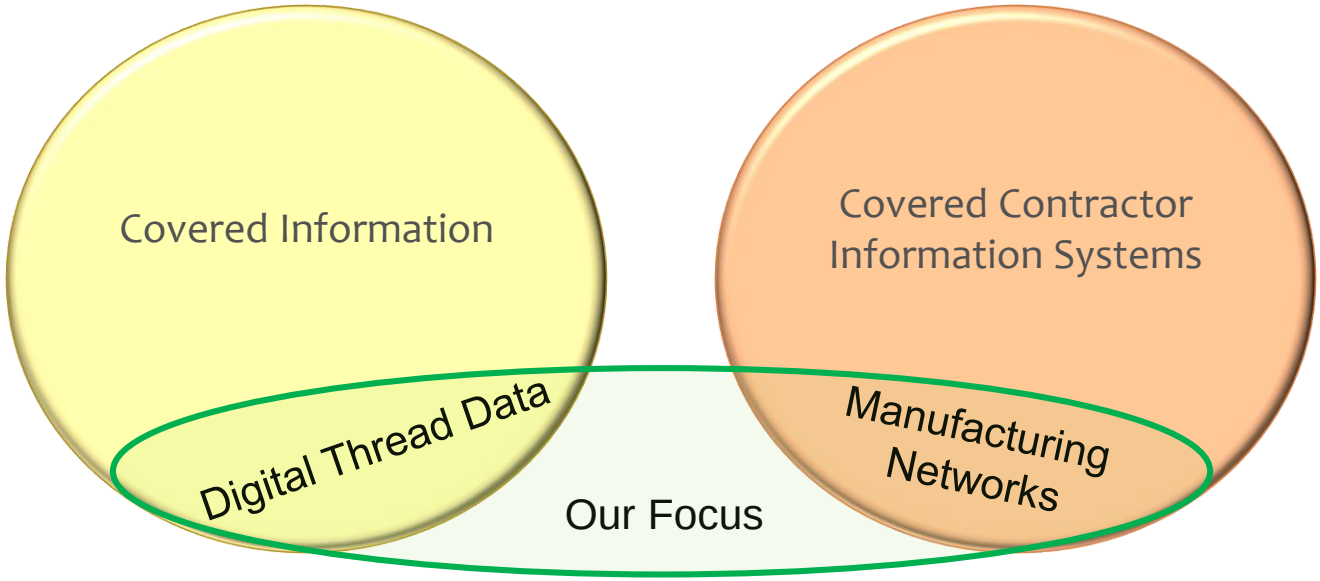
NDIA Cybersecurity Studies Timeline



Scope of Current Study

"Safeguarding Covered Defense Information and Cyber Incident Reporting" DFARS SUBPART 204.73

"Network Penetration" DFARS 252.204-7008 and 252.204-7012



Our recommendations will focus on:

Operational technology networks and interfaces, not IT or enterprise networks

Manufacturing cyber environment, not general cybersecurity

Operational Technology Environment

ICS systems are long-lived capital investments (15-20 year life)

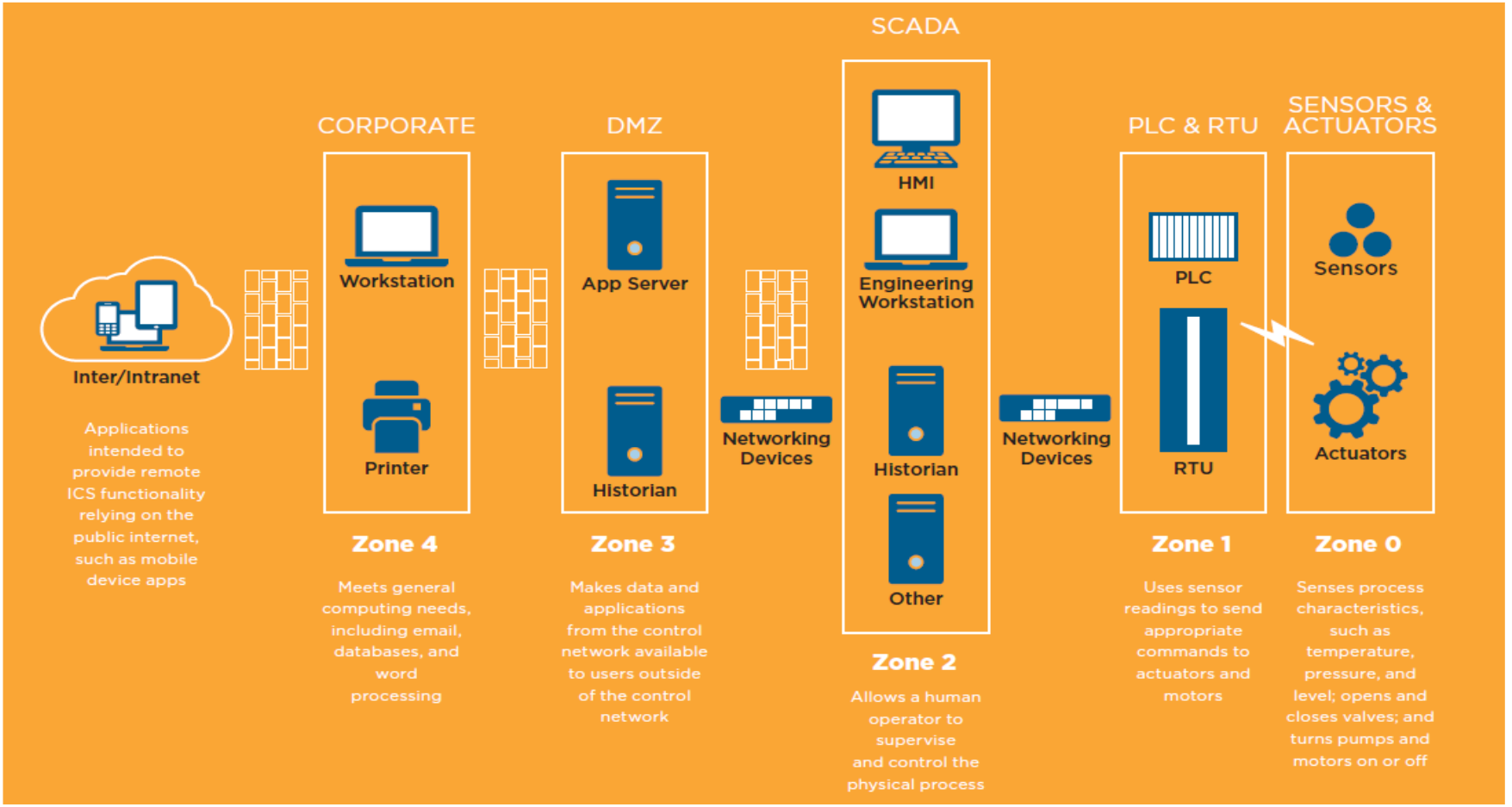
"Production mindset" with little tolerance for OT down time

Nascent cybersecurity awareness and limited workforce training

Manufacturing jobs bring executable code into system

IT Controls in NIST SP 800-171 do not directly fit OT Environment

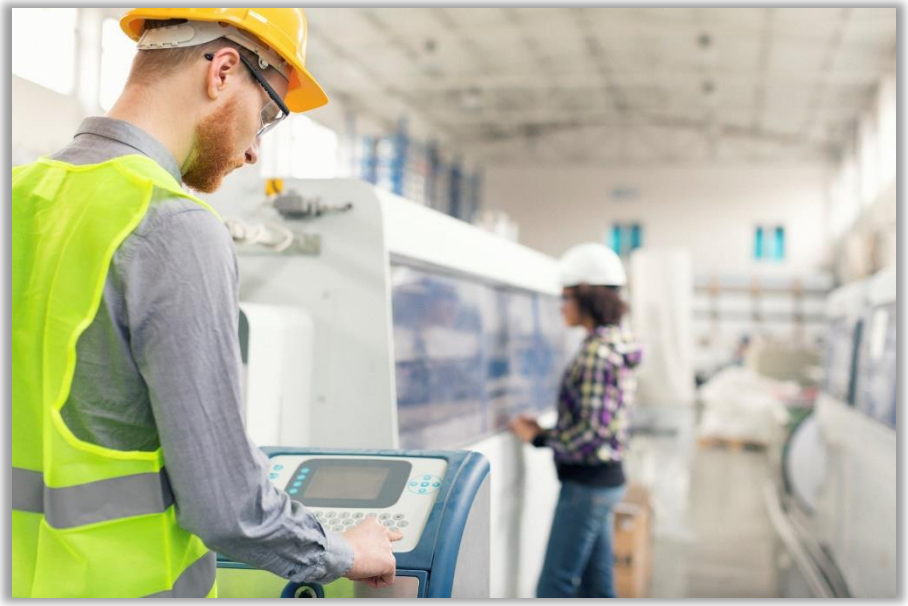
The Technical View



Source: *Overload: Critical Lessons Learned from 15 Years of ICS Vulnerabilities*, Fireeye Insight Intelligence 2016 Industrial Control Systems (ICS) Vulnerability Trend Report

Small and Mid-Size Enterprises (S&MEs)

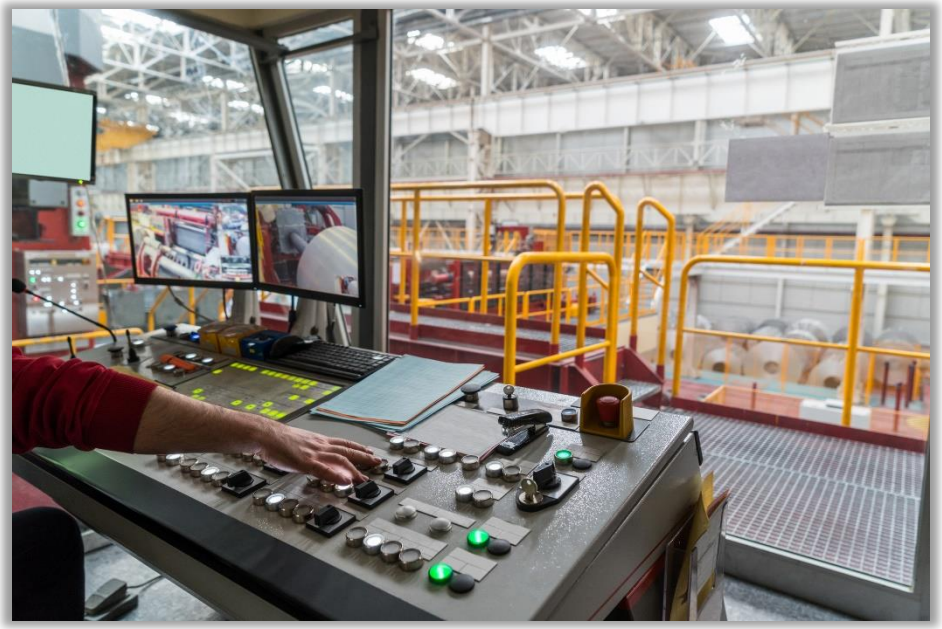
- Often lack cybersecurity knowledge and resources
- Most have no full time cybersecurity staff
- Believe they are not targets, so they focus on perimeter defense for IT network
- Many lack a business case for investing in OT cybersecurity



S&MEs are Critical to Defense Manufacturing

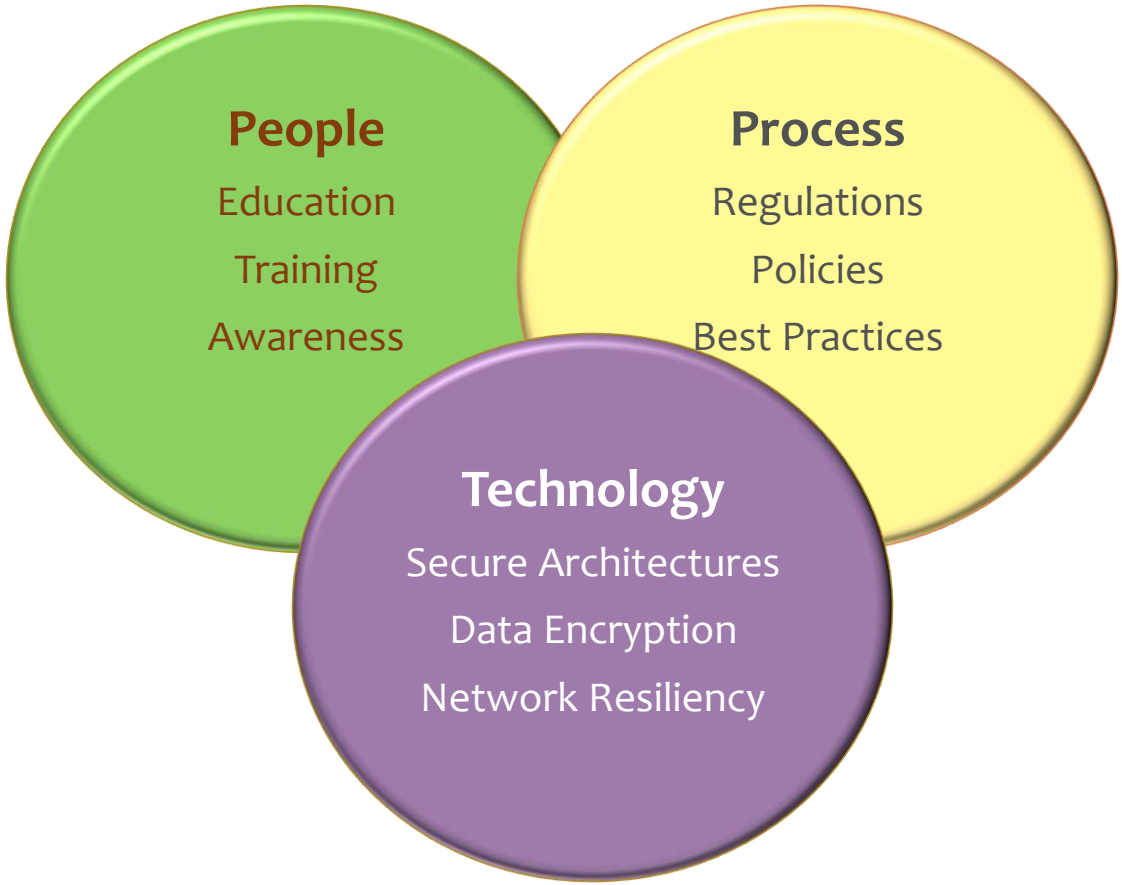
Need Solutions Specifically for OT Environment

- Training at all organizational levels
- Raising cybersecurity awareness with operators
- Incentives for improving cyber hygiene
- Implementing selected IT best practices
- Increasing interaction with IT network personnel and production engineers
- Including component security features in selection criteria



Viable shop floor concerns and priorities need to be understood and addressed to improve solution adoption

Following People-Technology-Process Triad



Preliminary Implementation Summary

1. Clarify DFARS requirements for manufacturing environment
2. Amend DoD guidance to include shop floor protections
3. Explore participation in IIoT standards development

4. Develop training programs for multiple constituencies
5. Develop manufacturing cybersecurity awareness campaign
6. Launch research and develop efforts to fill technical gaps

Incentives Will Be An Essential Component

Emerging R&D Recommendations

- Agile and flexible threat attribution/deterrent system
- Data protection, design and encryption technology
- Enterprise architecture and new technology concepts
- Hybrid cloud deployment
- Artificial intelligence, augmented reality

Next Steps

- Developing implementation steps for recommendations
- Engaging in outreach to share progress, validate findings, and continue information collection
- Formal report to be submitted to DoD in Summer 2017
- Joint working group members will continue to collaborate with DoD

Report will be coordinated within DoD, and other government agencies as appropriate, after new leadership team is in place

Contact Information:

Catherine J Ortiz, President
Defined Business Solutions, LLC

cjortiz@definedbusiness.com

804-462-0564
202-683-2021

Stock photos licensed from Getty Images

Backup Slides

What Should Small Manufacturers Do?

- Have an Integrated Cyber Incident Response Plan (see NIST SP 800-81r2)
  - Exercise this plan frequently
- Work with major customers to define requirements and get help
  - Take advantage of forthcoming NIST MEP help
- Become a smart buyer of products and services to:
  - Implement a defensible architecture
    - Segmentation
    - Hardened virtualization , especially for older operating systems
    - Two-factor authentication
    - Application whitelisting
    - Continuous network monitoring
  - Add ICS-specific security capabilities
    - Sensors on ICS ingress and egress points
    - Intrusion Detection and Prevention capabilities
    - Event log collection and analysis
    - Agents on Windows hosts to speed analysis

Manufacturing is an Inviting Target


The Washington Post

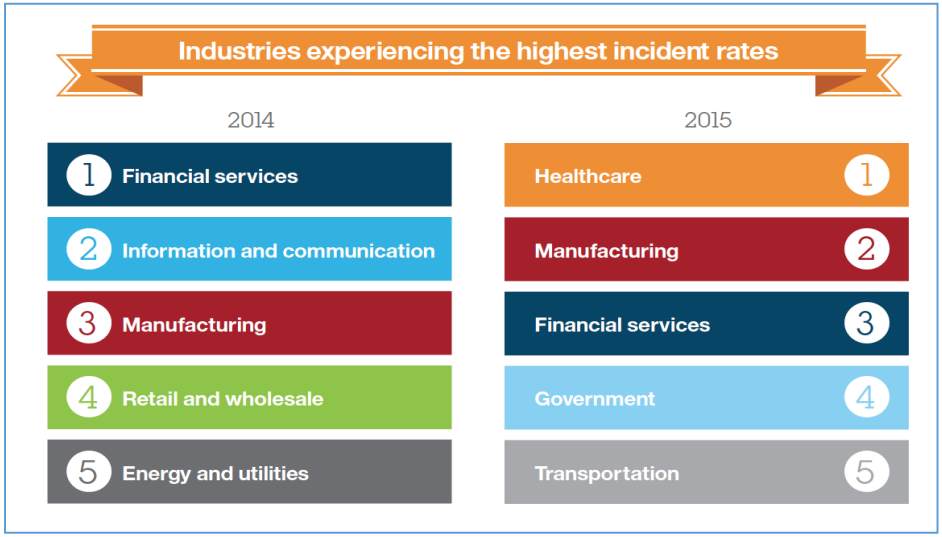
…Washington, DC May 28, 2013 Edition: U.S. | Regional Make us your

Weapons designs compromised by Chinese hackers

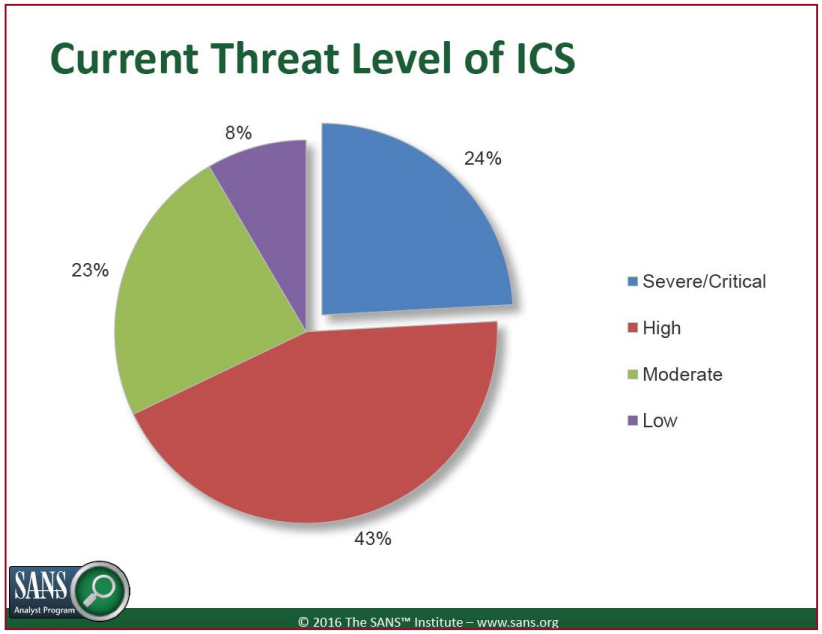
Ellen Nakashima 10:54 PM ET

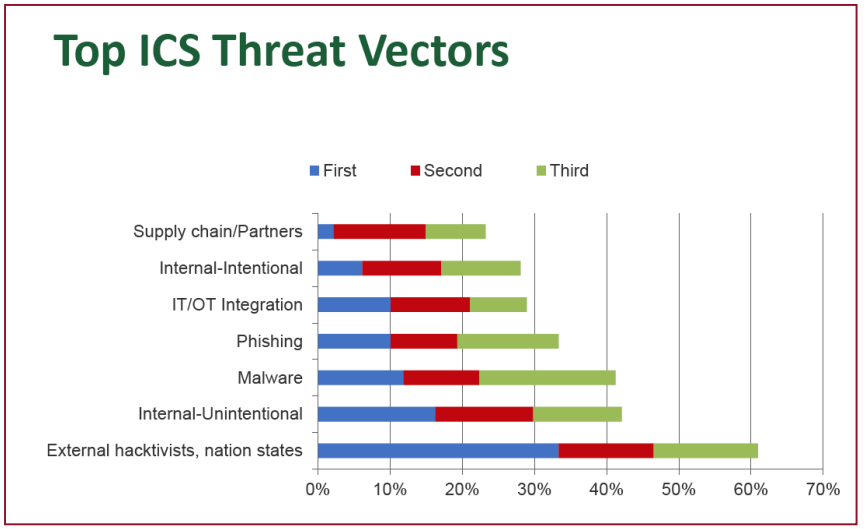
Among more than two dozen U.S. systems breached are programs critical to missile defenses and combat aircraft, according to a confidential report.

- List of compromised designs



IBM Security Services Cyber Security Intelligence Index 2016





SANS 2016 ICS Survey

March 8, 2017

2014 NDIA White Paper Recommendations for USD(AT&L)

1. Designate a focal point to work with industry on risk-based, voluntary standards and practices for factory floor cybersecurity.
   - Evaluate NIST framework as starting point.
2. Conduct forums with industry to help understand and implement DFARS clause, including factory floor implications.
3. Update DoD guidance on the Program Protection Plan (PPP). Let industry make appropriate risk/cost tradeoffs.
4. Use red teams to expose vulnerabilities, sponsor R&D to fill gaps
5. Assist SME suppliers with training and investments
   - NIST Manufacturing Extension Partnership to deliver training
   - Defense Prod Act Title III and Manufacturing Technology investments
   - Training for DoD contracting officers